SOLUZIONI DEL COMPITINO DEL 18/11/2014

Esercizio 1. Sia F il campo di spezzamento di $X^3 - 12 \in \mathbb{Q}[X]$ e sia $E = F(\zeta_5)$, dove $\zeta_5 := \exp(2\pi i/5)$.

(1) Al variare di $j \in \mathbb{N}$ si determini una base $\mathcal{B}_j$ di $\mathbb{Q}\left(\sqrt[3]{12}\zeta_3^j\right)$ su $\mathbb{Q}$, dove $\zeta_3 := \exp(2\pi i/3)$, e si mostri che $\mathbb{Q}\left(\sqrt[3]{12}\zeta_3^j\right) \subset F$.
(2) Si scriva $F = \mathbb{Q}(\alpha, \beta)$ con $\alpha, \beta \in \mathbb{C}$.
(3) Si determini una base $\mathcal{B}$ di $F/\mathbb{Q}$ e si scrivano gli elementi di $\mathcal{B}_j$ come combinazione $\mathbb{Q}$-lineare degli elementi di $\mathcal{B}$.
(4) Si mostri che $\mathbb{Q}\left(\sqrt[3]{12}\zeta_3^i\right) \neq \mathbb{Q}\left(\sqrt[3]{12}\zeta_3^j\right)$ se e solo se $i \neq j \mod 3$ e che, in questo caso

$$\mathbb{Q}\left(\sqrt[3]{12}\zeta_3^i\right) \cap \mathbb{Q}\left(\sqrt[3]{12}\zeta_3^j\right) = \mathbb{Q}.$$

(5) $(*)$ Si determini $G_{E/\mathbb{Q}}$ come gruppo astratto.

Soluzione: $(1-2)$ Se $\sqrt[3]{12}$ è l'unica radice reale di $f(X) := X^3 - 12$, l'insieme delle radici di $f(X)$ è

$$R_f = \left\{\sqrt[3]{12}, \sqrt[3]{12}\zeta_3, \sqrt[3]{12}\zeta_3^2\right\}.$$

Dunque $\mathbb{Q}\left(\sqrt[3]{12}\zeta_3^i\right) \subset \mathbb{Q}(R_f) =: F$. Vediamo anche che $F := \mathbb{Q}(R_f) \subset \mathbb{Q}\left(\sqrt[3]{12}, \zeta_3\right)$ e viceversa, poichè $\sqrt[3]{12} \in \mathbb{Q}(R_f)$ e $\zeta_3 = \frac{\sqrt[3]{12}\zeta_3}{\sqrt[3]{12}} \in \mathbb{Q}(R_f)$, si ha

$$F = \mathbb{Q}\left(\sqrt[3]{12}, \zeta_3\right).$$

Delle basi $\mathcal{B}_i$ sono le seguenti:

$$\begin{aligned}
\mathcal{B}_0 &= \left\{1, 12^{\frac{1}{3}}, 12^{\frac{2}{3}}\right\}, \\
\mathcal{B}_1 &= \left\{1, 12^{\frac{1}{3}}\zeta_3, 12^{\frac{2}{3}}\zeta_3^2\right\}, \\
\mathcal{B}_2 &= \left\{1, 12^{\frac{1}{3}}\zeta_3^2, 12^{\frac{2}{3}}\zeta_3^4 = 12^{\frac{2}{3}}\zeta_3\right\}.
\end{aligned}$$

(3) Si ha $\left[\mathbb{Q}\left(\sqrt[3]{12}\right) : \mathbb{Q}\right] = \deg(f) = 3$, poichè f è irriducibile per Eisenstin applicato al primo 3, e $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$. Una base $\mathcal{B}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}$ di $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ è data da $\{1, \zeta_3\}$ e quindi, poichè $\left[\mathbb{Q}\left(\sqrt[3]{12}\right) : \mathbb{Q}\right]$ e $[\mathbb{Q}(\zeta_3) : \mathbb{Q}]$ sono coprimi ed $F = \mathbb{Q}\left(\sqrt[3]{12}, \zeta_3\right)$, una base $\mathcal{B}$ si ottiene come segue:

$$\begin{aligned}
\mathcal{B} &= \left\{\alpha\beta : \alpha \in \mathcal{B}_0, \beta \in \mathcal{B}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}\right\} \\
&= \left\{1, 12^{\frac{1}{3}}, 12^{\frac{2}{3}}, \zeta_3, 12^{\frac{1}{3}}\zeta_3, 12^{\frac{2}{3}}\zeta_3\right\}.
\end{aligned}$$

Abbiamo $\mathcal{B}_0 \subset \mathcal{B}$ mentre $\mathcal{B}_1 - \mathcal{B} = \left\{12^{\frac{2}{3}}\zeta_3^2\right\}$ e $\mathcal{B}_2 - \mathcal{B} = \left\{12^{\frac{1}{3}}\zeta_3^2\right\}$. Usando la relazione ciclotomica $\zeta_3^2 = -1 - \zeta_3$ troviamo

$$12^{\frac{2}{3}}\zeta_3^2 = -12^{\frac{2}{3}} - 12^{\frac{2}{3}}\zeta_3 \text{ e } 12^{\frac{1}{3}}\zeta_3^2 = -12^{\frac{1}{3}} - 12^{\frac{1}{3}}\zeta_3.$$

Dunque

$$\begin{aligned}\mathcal{B}_0 &= \left\{1, 12^{\frac{1}{3}}, 12^{\frac{2}{3}}\right\},\\ \mathcal{B}_1 &= \left\{1, 12^{\frac{1}{3}}\zeta_3, -12^{\frac{2}{3}} - 12^{\frac{2}{3}}\zeta_3\right\},\\ \mathcal{B}_2 &= \left\{1, -12^{\frac{1}{3}} - 12^{\frac{1}{3}}\zeta_3, 12^{\frac{2}{3}}\zeta_3\right\}\end{aligned}$$

è una scrittura degli elementi di $\mathcal{B}_i$ come combinazione $\mathbb{Q}$-lineare degli elementi di $\mathcal{B}$.

(4) Poichè $\mathbb{Q}\left(\sqrt[3]{12}\zeta_3^i\right)/\mathbb{Q}$ è una estensione di grado 3, per moltiplicatività dei gradi

$$\mathbb{Q}\left(\sqrt[3]{12}\zeta_3^i\right) \cap \mathbb{Q}\left(\sqrt[3]{12}\zeta_3^j\right) = \mathbb{Q}$$

oppure

$$\mathbb{Q}\left(\sqrt[3]{12}\zeta_3^i\right) = \mathbb{Q}\left(\sqrt[3]{12}\zeta_3^i\right) \cap \mathbb{Q}\left(\sqrt[3]{12}\zeta_3^j\right) = \mathbb{Q}\left(\sqrt[3]{12}\zeta_3^j\right)$$

ed ovviamente si ha la seconda opzione se $i = j \mod 3$ perchè allora $\mathbb{Q}\left(\sqrt[3]{12}\zeta_3^i\right) = \mathbb{Q}\left(\sqrt[3]{12}\zeta_3^j\right)$. Se viceversa $i \neq j \mod 3$ ed $i = 0$, uno dei due campi è contenuto in $\mathbb{R}$ mentre l'altro contiene $\sqrt[3]{12}\zeta_3^j \notin \mathbb{R}$. Dunque non possono coincidere e l'intersezione è $\mathbb{Q}$ per quanto notato. Se $i = 1$ e $j = 2$, $\mathbb{Q}\left(\sqrt[3]{12}\zeta_3\right) \neq \mathbb{Q}\left(\sqrt[3]{12}\zeta_3^2\right)$ poichè, ad esempio,

$$12^{\frac{1}{3}}\zeta_3 \in \mathbb{Q}\left(\sqrt[3]{12}\zeta_3\right) - \mathbb{Q}\left(\sqrt[3]{12}\zeta_3^2\right).$$

Se infatti $12^{\frac{1}{3}}\zeta_3 \in \mathbb{Q}\left(\sqrt[3]{12}\zeta_3^2\right)$, per (3) esisterebbero $a, b, c \in \mathbb{Q}$ tali che

$$\begin{aligned}12^{\frac{1}{3}}\zeta_3 &= a + b\left(-12^{\frac{1}{3}} - 12^{\frac{1}{3}}\zeta_3\right) + c12^{\frac{2}{3}}\zeta_3\\ &= a - b12^{\frac{1}{3}} - b12^{\frac{1}{3}}\zeta_3 + c12^{\frac{2}{3}}\zeta_3.\end{aligned}$$

Dall'unicità della scrittura come combinazione $\mathbb{Q}$-linear in funzione della base $\mathcal{B}$ seguirebbe $a = c = 0$ e quindi $0 = b = -1$. (Alternativamente, se $K := \mathbb{Q}\left(\sqrt[3]{12}\zeta_3\right) = \mathbb{Q}\left(\sqrt[3]{12}\zeta_3^2\right)$,

$$\zeta_3 = \zeta_3^{2-1} = \frac{\sqrt[3]{12}\zeta_3^2}{\sqrt[3]{12}\zeta_3} \in K$$

e quindi $\sqrt[3]{12} = \frac{\sqrt[3]{12}\zeta_3}{\zeta_3} \in K$. This is no possible because then $K = \mathbb{Q}\left(\sqrt[3]{12}, \zeta_3\right) = F$ avrebbe grado 6 su $\mathbb{Q}$).

(5) Poichè $F/\mathbb{Q}$ e $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ sono di Galois ed $E = F \cdot \mathbb{Q}(\zeta_5)$,

$$G_{E/\mathbb{Q}} \xrightarrow{\sim} \left\{(\sigma_1, \sigma_2) \in G_{F/\mathbb{Q}} \times G_{\mathbb{Q}(\zeta_5)/\mathbb{Q}} : \sigma_{1|F\cap\mathbb{Q}(\zeta_5)} = \sigma_{2|F\cap\mathbb{Q}(\zeta_5)}\right\}.$$

Notiamo che $\#G_{F/\mathbb{Q}} = 6$ e $G_{F/\mathbb{Q}}$ non può essere abeliano poichè $\mathbb{Q}\left(\sqrt[3]{12}\right) \subset F$ ma $\mathbb{Q}\left(\sqrt[3]{12}\right)/\mathbb{Q}$ non è una estensione normale: infatti $\mathbb{Q}\left(\sqrt[3]{12}\right) \subset \mathbb{R}$ contiene la radice reale $\sqrt[3]{12}$ di $f(X)$ ma non $\sqrt[3]{12}\zeta_3 \notin \mathbb{R}$. Dunque $G_{F/\mathbb{Q}} \simeq S_3$ e, d'altra parte, $G_{\mathbb{Q}(\zeta_5)/\mathbb{Q}} \simeq \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$ per la teoria dei campi ciclotomici.

Per moltiplicatività dei gradi,

$$[F \cap \mathbb{Q}(\zeta_5) : \mathbb{Q}] \mid ([F : \mathbb{Q}], [\mathbb{Q}(\zeta_5) : \mathbb{Q}]) = (6, 4) = 2.$$

Mostriamo che $[F \cap \mathbb{Q}(\zeta_5) : \mathbb{Q}] = 2$ non è possibile, da cui

$$G_{E/\mathbb{Q}} \xrightarrow{\sim} S_3 \times \frac{\mathbb{Z}}{4\mathbb{Z}}.$$

Il discriminante di $f(X)$ è $-27 \cdot 12^2$ la cui radice quadrata è $36i\sqrt{3}$: dunque $\mathbb{Q}\left(i\sqrt{3}\right) \subset F$ è l'unica estensione quadrata contenuta in F. D'altra parte, utilizzando la relazione ciclotomica

$\zeta_5^4 = -\zeta_5^3 - \zeta_5^2 - \zeta_5 - 1$ nella penultima delle seguenti uguaglianze, vediamo che

$$\begin{aligned}\left(\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4\right)^2 &= \zeta_5^2 + \zeta_5^4 + \zeta_5^6 + \zeta_5^8 \\ &\quad -2\zeta_5^3 - 2\zeta_5^4 + 2\zeta_5^5 + 2\zeta_5^5 - 2\zeta_5^6 - 2\zeta_5^7 \\ &= \zeta_5^2 - 2\zeta_5^3 - \zeta_5^4 + 4\zeta_5^5 - \zeta_5^6 - 2\zeta_5^7 + \zeta_5^8 \\ &= \zeta_5^2 - 2\zeta_5^3 - \zeta_5^4 + 4 - \zeta_5 - 2\zeta_5^2 + \zeta_5^3 \\ &= \zeta_5^2 - 2\zeta_5^3 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 + 4 - \zeta_5 - 2\zeta_5^2 + \zeta_5^3 \\ &= 5.\end{aligned}$$

Poichè $G_{\mathbb{Q}(\zeta_5)/\mathbb{Q}}$ è ciclico, da ciò segue che $\mathbb{Q}\left(\sqrt{5}\right) \subset \mathbb{Q}\left(\zeta_5\right)$ è l'unica estensione quadratica in $\mathbb{Q}\left(\zeta_5\right)$. Se dunque $[F \cap \mathbb{Q}\left(\zeta_5\right) : \mathbb{Q}] = 2$,

$$\mathbb{Q}\left(i\sqrt{3}\right) = F \cap \mathbb{Q}\left(\zeta_5\right) = \mathbb{Q}\left(\sqrt{5}\right),$$

dovendo $F \cap \mathbb{Q}\left(\zeta_5\right)$ essere contemporaneamente l'unica estensione quadratic in F ed in $\mathbb{Q}\left(\zeta_5\right)$. Ma ciò non è possibile poichè $\mathbb{Q}\left(\sqrt{5}\right) \subset \mathbb{R}$ mentre $i\sqrt{3} \notin \mathbb{R}$.

Esercizio 2. Sia $L = \mathbb{Q}\big(\zeta_{36}\big)$, con $\zeta_{36} = \exp^{\frac{2\pi i}{36}}$ il 36^o-campo ciclotomico.

(1) Si dimostri che $\mathbb{Q} \subset L$ è una estensione di Galois e se ne determini il grado.
(2) Si determini il gruppo di Galois $G = \mathrm{Gal}(L/\mathbb{Q})$. Si mostri che è abeliano. $(*)$ È ciclico?
(3) Si dimostri che esiste una estensione intermedia $\mathbb{Q} \subset K \subset L$ di grado 3 su $\mathbb{Q}$. $(*)$ È unica?
(4) [Teo] Si dica se ζ_{36} è costruibile con riga e compasso a partire da $A = \mathbb{Q}$ oppure da $A = K$.

Soluzione:

1) Il campo L risulta essere il campo di spezzamento del polinomio $X^{36} - 1 \in \mathbb{Q}[X]$. Infatti le sue radici sono $\mu_{36} := \{\zeta_{36}^j | j = 0, \ldots, 35\}$. Essendo $\mathbb{Q}$ un campo perfetto, il polinomio $X^{36} - 1$ risulta separabile e quindi $\mathbb{Q} \subset L$ è una estensione di Galois. Il grado è $\varphi(36) = \varphi(9)\varphi(4) = 4 \cdot 3 = 12$.

2) Osservo che μ_{36} è un sottogruppo ciclico di ordine 36 del gruppo moltiplicativo $\mathbb{C}^*$. In particolare $\mu_{36} \cong \mathbb{Z}/36\mathbb{Z}$ come gruppo e il abbiamo una identificazione del gruppo deli automorfismi (di gruppo) $\mathrm{Aut}(\mu_{36}) \cong \mathrm{Aut}\big(\mathbb{Z}/36\mathbb{Z}\big) \cong \big(\mathbb{Z}/36\mathbb{Z}\big)^*$.

L'omomorfismo $\rho\colon G \to \mathrm{Aut}(\mu_{36})$ che associa ad un automorfismo σ di L la sua restrizione $\sigma|_{\mu_{36}}$ a μ_{36} è un omomorfismo di gruppi, iniettivo visto che L è generato da ζ_{36} come estensione di $\mathbb{Q}$. Visto che la cardinalità di $\big(\mathbb{Z}/36\mathbb{Z}\big)^*$ è $\varphi(36) = 12$ allora ρ è un isomorfismo. Osservo inoltre che $\mathbb{Z}/36\mathbb{Z} \cong \big(\mathbb{Z}/9\mathbb{Z}\big) \times \big(\mathbb{Z}/4\mathbb{Z}\big)$ come anelli e quindi $\big(\mathbb{Z}/36\mathbb{Z}\big)^* \cong \big(\mathbb{Z}/9\mathbb{Z}\big)^* \times \big(\mathbb{Z}/4\mathbb{Z}\big)^*$. Inoltre $\big(\mathbb{Z}/4\mathbb{Z}\big)^*$ e quindi isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Il gruppo $\big(\mathbb{Z}/9\mathbb{Z}\big)^*$ è abeliano di ordine 6 e quindi isomorfo a $\mathbb{Z}/6\mathbb{Z} = \big(\mathbb{Z}/2\mathbb{Z}\big) \times \big(\mathbb{Z}/3\mathbb{Z}\big)$. Deduco quindi che

$$G \cong \big(\mathbb{Z}/3\mathbb{Z}\big) \times \big(\mathbb{Z}/2\mathbb{Z}\big) \times \big(\mathbb{Z}/2\mathbb{Z}\big).$$

In particolare è abeliano ma non ciclico. Se fosse ciclico esisterebbe un elemento di ordine 12 mentre ogni elemento ha ordine al più 6

3) Osserviamo dalla descrizione di G che esiste un quoziente G/H isomorfo a $\mathbb{Z}/3\mathbb{Z}$. Per il teorema fondamentale della teoria di Galois ho che $K := L^H$ è una estensione di grado 3 di $\mathbb{Q}$. Tale estensione è anche unica in quanto H è un 2 Sylow di G e, visto che i 2 Sylow sono tutti coniugati e che G è abelaino, esiste un unico sottogruppo di G di ordine 4.

4) Se ζ_{36} fosse costruibile con riga e compasso a partire da $\{0, 1\}$, allora l'estensione $\mathbb{Q} \subset L$ avrebbe grado una potenza di 2 e questo non è vero. Invece ζ_{36} risulta costruibile con riga

e compasso a partire da K in quanto l'estensione $K \subset L$ è di Galois con gruppo di Galois $H = \mathrm{Gal}(L/K)$ isomorfo al gruppo di Klein. Prendendo gli invarianti di un sottogruppo di ordine 2 troviamo una estensione intermedia $K \subset E \subset L$ tale che $[E : K] = 2 = [L : E]$. L'affermazione segue allora dalla caratterizzazione dei numeri costruibili acon riga e compasso a partire da K come numeri contenuti in estensioni finite di K che si possono scrivere come estensioni quadratiche successive.

Esercizio 3 (Teo)**.** Sia $f(X) \in \mathbb{F}_p[X]$ un polinomio irriducibile e sia $n \in \mathbb{N}_{\geq 1}$. Si mostri che i seguenti fatti sono equivalenti.

(1) $f(X) \in \mathbb{F}_{p^n}[X]$ ammette una radice.
(2) $f(X) \in \mathbb{F}_{p^n}[X]$ si spezza completamente.
(3) $\deg(f) \mid n$.

Soluzione: Per cominciare notiamo che, poichè $f(X) \in \mathbb{F}_p[X]$ è irriducibile,

$$E_f := \frac{\mathbb{F}_p[X]}{\mathbb{F}_p[X] f(X)}$$

è un campo tale che $[E_f : \mathbb{F}_p] = \deg(f)$, ovvero $\#E_f = p^{\deg(f)}$. Per definitione $f(X) \in E_f[X]$ ammette $X + \mathbb{F}_p[X] f(X)$ come radice e, poichè dallo studio dei campi finiti sappiamo che $E_f/\mathbb{F}_p$ è una estensione normale, concludiamo che E_f è il campo di spezzamento di $f(X)$. In altre parole, il campo di spezzamento di $f(X)$ è $E_f = \mathbb{F}_{p^{\deg(f)}}$, dove $\mathbb{F}_{p^{\deg(f)}}$ denota l'unico campo finito con $p^{\deg(f)}$ elementi. Dallo studio dei campi finiti sappiamo che $\mathbb{F}_{p^{\deg(f)}} \subset \mathbb{F}_{p^n}$ se e solo se $\deg(f) \mid n$ e ciò mostra (2) $\Leftrightarrow$ (3). D'altra parte l'equivalenza (1) $\Leftrightarrow$ (2) segue dalla osservazione che $\mathbb{F}_{p^n}/\mathbb{F}_p$ è una estensione normale.